<u>REMARKS</u>

The present application has been reviewed in light of the Office Action dated

August 1, 2008. Claims 1-7 and 10 are presented for examination, of which Claims 1, 7, and 10

are independent form. Claims 1-3, 6, 7, and 10 have been amended to define aspects of

Applicant's invention more clearly. Favorable consideration is requested.

The Office Action states that Claims 1, 6, 7, and 10 are rejected under 35 U.S.C.

§ 103(a) as being unpatentable over U.S. Patent No. 6,938,154 (*Berson et al.*) in view of U.S.

Patent Application Publication No. 2003/0043416 (*Rublee et al.*); that Claim 2 is rejected under

35 U.S.C. § 103(a) as being unpatentable over *Berson et al.* and *Rublee et al.* in view of and U.S.

Patent No. 7,117,493 (*Matasushima*); that Claims 3 and 4 are rejected under 35 U.S.C. § 103(a)

as being unpatentable over *Berson et al.*, *Rublee et al.,* and *Matasushima* in view of U.S. Patent

No. 7,158,657 (*Okazaki et al.*); and that Claim 5 is rejected under 35 U.S.C. § 103(a) as being

unpatentable over *Berson et al.*, *Rublee et al.*, *Matasushima*, and *Okazaki* in view of U.S. Patent

Application Publication No. 2003/0163730 (*Roskind et al.*). For at least the reasons presented

below, Applicant submits that independent Claims 1, 7, and 10, together with the claims

dependent therefrom, are patentably distinct from the cited prior art.

Claim 1 is directed to an authentication method of an image processing system in

which a host computer, an authentication apparatus, and an image processing apparatus are

connected to a network. A first request for authentication is issued from the host computer to the

image processing apparatus, when the host computer remotely operates the image processing

apparatus. In response to the first request, the host computer receives from the image processing

apparatus data specifying the authentication apparatus, which authenticates an operation level of

6

a remote operation. The host computer issues to the authentication apparatus a second request

for an authentication process, which is based on the data transmitted by the image processing

apparatus. The authentication process is to authenticate an operation level of the remote

operation performed by the host computer. The host computer remotely operates the image

processing apparatus in accordance with the operation level authenticated by the authentication

process.

Notable features of Claim 1 "a reception step of, at the host computer, receiving

from the image processing apparatus data for specifying the authentication apparatus, which

authenticates an operation level of a remote operation, in response to the request in the first

request step, wherein the authentication process is to authenticate an operation level of the

remote operation performed by the host computer." By virtue of these features, the host

apparatus facilities the operation of the image processing apparatus, because the image

processing apparatus does not authenticate the operation level of the remote operation performed

by the host computer; instead the image processing apparatus provides the host apparatus with

data specifying an authentication apparatus, for example.[1]

Berson et al. relates to identification, management, and operation of network

devices. FIG. 3 of *Berson et al.* illustrates a process for secure operation of a network device,

such as a printer, a copier, a scanner, or a facsimile machine. As understood by Applicant, a

digital certificate is assigned to a network user, which can be a person or another network device.

The digital certificate is associated with a command for operation of a network device. When the

---

[1] The example(s) presented herein are intended for illustrative purposes only. Any details
presented in the illustrative example(s) should not be construed to limit the scope of the claims.

command for operation of the network device is received, a determination is made whether any usage policy applies to the user or to the network device. If authentication of the network device is required, a digital certificate of the network device is authenticated, and the digital certificate of the network user also is authenticated. Operation of the network device is enabled after successful authentication. Notably, nothing has been found in *Berson et al.* that is believed to teach or suggest an authentication process that authenticates <u>an operation level</u> of a remote operation performed by a host computer.

    Rublee et al. relates to a system for scanning hard-copy images to electronic mail addresses. As understood by Applicant, *Rublee et al.* discloses a scanner that sends a host name of an authentication server to a domain name server, which responds by sending a corresponding address of the authentication server to the scanner (see page 3, paragraph 25). When a user of the scanner logs into the network, the scanner then sends an authentication request to the authentication server, which responds to the scanner with an indication of whether the user has been successfully authenticated. The scanner, however, does not remotely operate the domain name server. Moreover, as best understood by Applicant, neither the scanner, the domain name server, nor the authentication server authenticates <u>an operation level</u> of a remote operation performed by a host computer.

    Based on the foregoing remarks, Applicant submits that a combination of *Berson et al.* and *Rublee et al.*, assuming such combination would even be permissible, would fail to teach or suggest an authentication method that includes "a reception step of, at the host computer, receiving from the image processing apparatus data for specifying the authentication apparatus, which authenticates an operation level of a remote operation, in response to the request in the

8

first request step, wherein the authentication process is to authenticate an operation level of the remote operation performed by the host computer," as recited in Claim 1. Accordingly, Applicant submits that Claim 1 is patentable over *Berson et al.* and *Rublee et al.*, and respectfully requests withdrawal of the rejection under 35 U.S.C. § 103(a).

Independent Claims 7 and 10 include features similar to those discussed above, in which an operation level of a remote operation is authenticated based on data from an image processing apparatus. Therefore, those claims are believed to be patentable for at least the reasons discussed above. The other rejected claims in this application depend from one or another of the independent claims discussed above and, therefore, are submitted to be patentable for at least the same reasons. Because each dependent claim also is deemed to define an additional aspect of the invention, individual consideration of the patentability of each claim on its own merits is respectfully requested.

No petition to extend the time for response to the Office Action is deemed necessary for this Amendment. If, however, such a petition is required to make this Amendment timely filed, then this paper should be considered such a petition and the Commissioner is authorized to charge the requisite petition fee to Deposit Account 06-1205.

CONCLUSION

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable consideration and an early passage to issue of the present application.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

/Lock See Yu-Jahnes/
Lock See Yu-Jahnes
Attorney for Applicants
Registration No. 38,667

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

FCHS_WS 2437574v2